



AF / 3651
120

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

RECEIVED

AUG 20 2004

GROUP 3600

In re application of: Leon Saltsov, et al.

Serial or Patent No.: 09/503,122

For: VALIDATOR WITH REMOVABLE FLASH MEMORY

Filed: February 14, 2000

Group Art Unit: 3651

Attorney Docket No.: WH-10 752US

133 Richmond Street West
Toronto, Ontario M5H 2L7

BY COURIER

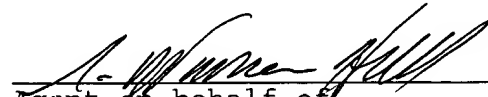
The Commissioner of Patents and Trademarks, August 16, 2004
Washington, D.C. 20231
U.S.A.

Dear Sir:

This is in response to the Communication dated July 19, 2004 from the Examiner regarding the Notification of Non Compliance with the requirements of 37 C.F.R. 1.192(c).

Attached is a revised Appeal Brief in triplicate which includes the identification of the issue with respect to 35 U.S.C. 102(e) based on Meyer et al. and arguments that the rejection of claim 6 on this basis, is in error.

Respectfully submitted,


Agent on behalf of
Applicant
S. Warren Hall
Reg. No. 30,350
(416) 368-8313

WH/sdw

Enclosures



THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of: Leon Saltsov, et al.
Serial or Patent No.: 09/503,122
For: VALIDATOR WITH REMOVABLE FLASH MEMORY
Filed: February 14, 2000
Group Art Unit: 3651

Attorney Docket No.: WH-10 752US 133 Richmond Street West
Toronto, Ontario M5H 2L7

August 16, 2004

BY COURIER

The Commissioner of Patents and Trademarks
Washington, D.C. 20231
U.S.A.

Dear Sir:

APPEAL BRIEF

On May 23, 2002 the appellant appealed the final rejection of claims 1 through 6, 8, and 10 through 20. An amended Appeal Brief was filed on April 10, 2003. On July 19, 2004, a Notice of Non-Compliance was issued. What follows is appellant's Appeal Brief as required by 37 C.F.R. 1.92(a) that addresses the issues raised in the Notice of Non-Compliance.

REAL PARTY OF INTEREST

The real party of interest is CashCode Company Inc. An assignment document transferring all rights from the inventors to CashCode Company Inc. was filed with the Patent Office on February 14, 2000.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences which will directly affect or be affected by the present appeal.

STATUS OF THE CLAIMS

Claims 1 through 6, 8, and 10 through 20, have been rejected. Claims 7 and 9 were cancelled in the response of November 19, 2001.

STATUS OF THE AMENDMENTS

Proposed amendments filed in the response of April 25, 2002 and the Voluntary Amendment of August 22, 2002 were not entered as the Examiner asserted the claims raised new issues.

SUMMARY OF THE PRESENT INVENTION

The present invention provides a cost effective arrangement for updating of the algorithms and software of banknote validators using a removable memory storage arrangement. The validator provides positive confirmation that the removable memory storage arrangement being used to update the validator is authorized. This security is highly desirable as the validator is accepting and/or rejecting banknotes provided as payment for products or services. If a fraudulent banknote is accepted, the provider of the product or service is the victim of a theft.

Corruption or replacement of the software and algorithms used to evaluate banknotes with unauthorized software or algorithms could result in an updated validator accepting banknotes that should have been rejected.

Updating of validators is necessary to recognize new banknotes, or to use improved evaluation techniques, or to identify known fraudulent banknotes. Unfortunately, the quality of fraudulent banknotes is continuously improving, leaving older validators vulnerable.

Updating of validators in the field by technicians replacing the software without inherent security leaves the validators vulnerable. Returning of validators to a service center is not convenient or cost effective. Updating by direct connection to a central computer which then downloads software in a secure manner is not practical as the validators do not have this communication capability and would be time consuming for a qualified technician to temporarily provide this capability.

Banknote validators are often part of the payment receiving capability of a vending machine or other dispensing device in non supervised locations. Locations of this type increase the risk of possible sabotage.

To overcome these disadvantages, the validator of the present invention includes a central processing unit which has a test procedure that evaluates the integrity of the removable memory storage arrangement when received in the validator. The information contained in the removable memory storage arrangement is only used upon positive evaluation of the memory storage arrangement by the central processing unit. With this arrangement, a banknote validator can be updated in a simple manner without skilled labour while the integrity of the validator is maintained. This self evaluation by the validator does not require remote communication which is impractical for many of these devices.

In a preferred embodiment, the validator includes decryption software for evaluating the integrity of software received in the removable memory storage arrangement and to be downloaded to the validator. The removable memory storage arrangement includes an electronic address which is additionally coded with the encrypted algorithms. The validator uses the

decryption software and the electronic address of the removable memory storage arrangement to compare the electronic address with the electronic address that was encrypted with the algorithms of the removable memory storage arrangement. If there is a match the process is considered to be authorized and the validator is updated. If there is no match then the process stops. With this arrangement the validator, which could have been manufactured many years earlier, has decryption software and a process for evaluating a removable memory storage arrangement when inserted in the validator. The removable memory storage arrangement has this address information as well as the coded address information which is used by the validator using the decryption software to confirm the authenticity of the removable memory storage arrangement. Thus security and integrity of the validator is maintained by the particular cooperation between the validator and the removable memory storage arrangement. There is no requirement to contact a central server and no requirement to provide the validator with the ability to communicate with the central server. Tampering of the encrypted algorithms is difficult and is highly likely to corrupt the encoded electronic address. Therefore, security is provided in a simple cost effective manner.

With this security arrangement, the removable flash memory device can be used by any suitable validator. The removable flash memory device has a particular structure with a read only memory and a rewritable memory containing encrypted operating software that also contains an encryption of the identification code contained in the read only memory. Thus, the security is contained in the removable flash memory device. The validator uses its encryption software to evaluate the integrity of an inserted flash memory device, based on the information contained therein. In this way, the removable flash memory

device is suitable for updating of any validator of the appropriate type.

Figure 1 shows the banknote validator 2 with the preferred removable flash memory 20. Figure 2 shows the interface between the removable flash memory and the CPU of the validator. Figure 3 shows the design of the removable flash memory device and its serial number which is fixed. This serial number is additionally encrypted as part of the encrypted software of the flash memory device and is compared by the validator with the fixed serial number. Figure 5 provides details of the security steps carried out by the validator when a removable flash memory device is inserted. Figure 6 shows the removable sensors used to evaluate banknotes. Replacement sensor modules can also be part of the updating of the validator.

Independent claim 6 is directed to a serial flash memory module, having a read only memory and a rewritable memory. The identification code of the module is provided in the read only memory while the rewritable memory contains encrypted validator software and encryption of at least part of the identification used to confirm the integrity of the module.

In a preferred embodiment as defined in dependent claim 8, the removable memory storage arrangement after updating of the validator is used by the validator as additional memory.

Dependent claim 12 is directed to a security feature of the removable memory storage arrangement where it can only be used once. In this way further control of the security of the validators and the updating of validators is maintained by the manufacturer.

Dependent claim 13 defines the matching of the removable memory storage arrangement with the validator by providing the validator's serial number to the removable memory storage arrangement.

Claim 16 is limited to the updating of software and removable sensors where the update requires both new sensors and software. Dependent claim 18 requires replaceable sensor modules (see figure 6 and 7).

ISSUES

Claim 6 is rejected under 35 U.S.C. 102(e) as anticipated by Meyer et al., United States Patent 6,301,344.

Claims 1 through 6, 8 and 10 through 15 are rejected under 35 U.S.C. 103(a) in light of Mazur et al, United States Patent 6,241,069 in view of Meyer et al. United States Patent 6,301,344.

Claims 16 - 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mazur et al in view of Itako et al.

Claims 19 is rejected under 35 U.S.C. 103(a) in light of Mazur et al, United States Patent 6,241,069, in view of Meyer et al United States Patent 6,301,344 further in view of Itako et al United States Patent 5,964,336.

Claims 16 - 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mazur et al in view of Meyer et al and further in view of Itako et al.

Claims 1 - 20 are rejected under the judicially created doctrine of double patenting in light of claims 1 - 18 of US Patent 6,142,284 in view of Meyer et al.

GROUPING OF THE CLAIMS

Claims 1 through 6, 8, and 10 through 20, do not fall together.

Each claim stands independent of the other claims as it includes additional limitations which together with the limitations of the primary claim patentably distinguish over the structures.

In particular, independent claims 1, 6, and 19 are separate as the elements of the combination are different as argued below. The subject matter of these claims is completely different. Dependent claims 3 and 5 are separate and distinct from claim 1 as a particular structure for encrypting is defined whereas claim 1 is directed to the broader concept of a test procedure being used to evaluate the integrity of the removable memory storage arrangement.

ARGUMENTS

Rejection under 35 U.S.C. 102(e).

The rejection of claim 6 as rejected under 35 U.S.C. 102(e) as being anticipated by Meyer et al. is traversed.

Claim 6 requires a serial flash memory module for updating a validator and comprises a read only memory having an identification code specific to the serial flash memory module and a rewritable memory containing encrypted operating software for operating a validator. In addition, the encrypted software

includes encryption of at least part of the identification code. With this arrangement, the serial flash memory module can be checked for authenticity. Tampering of the encrypted operating software contained in the rewritable memory is also likely to alter the encrypted portion of the identification code. As outlined in the application, the validator only updates its operating system when the appropriate match is present.

The rejection under 35 U.S.C. 102(e) based on Meyer is believed to be deficient. The Examiner relies on column 17 of the patent, lines 40 - 47 which refers to a read only memory of the telephone, which includes an ID code from 0 to 63 that is specific to the integrated circuit of the telephone. A rewritable memory only contains the "unique key" of the telephone. The ID code and the "unique key" are used to generate a soft key that can be used to encrypt information stored by the telephone. The Examiner states that this encrypted information could include the ID code but there is no teaching of this in the application and no teaching to store such encrypted ID code in the rewritable memory of the serial flash memory module as required by claim 6.

The portion of the Meyer reference referred to by the Examiner (column 17, lines 40 through 54) is directed to the generation of a soft key used to allow the phone to confirm that tampering thereof has not occurred. The phone, to generate the soft key, requires two different pieces of information. It requires a "seed" which is an identification code corresponding to a number between 0 - 63 which is fixed in the six bit register of a custom integrating circuit. In addition to this seed, the device of Meyer includes a flash memory device where a serial number of the telephone is provided. As noted in the application, this serial number could be copied or changed.

The device uses the seed, i.e., the I.D. number from 0 - 63, in combination with the serial number contained in the rewritable memory to generate a soft key. Each time the device is initiated, the device uses the seed and serial number of generate a soft key which is then used to compare to a previously compared soft key. If a match occurs, then it is believed that no change has been made to the serial number and to the reporting of the device. This soft key can also be used to encrypt information to be stored by the telephone. Typical applications of the soft key are stated in column 17, line 65 to column 18, line 25. These applications are unrelated to the claimed subject matter.

It is apparent that the Meyers et al. structure does not have a serial flash memory module containing a read only memory which includes an identification code specific to the flash memory module, in combination with a rewritable memory containing encrypted operating software for operating a validator. There is no encrypted operating software as specifically required by the claim contained in the rewritable memory of the serial flash memory module. Furthermore, there is no teaching of including within this encrypted software at least part of the identification code contained in the read only memory.

The Meyer et al. structure is designed to provide security to a remote telephone device. One problem associated with such telephone device is the serial number of the device could be tampered with in order to avoid the payment of services. To overcome this, and to confirm that the serial number has not been tampered with, the generation of the soft key is completed and this generated soft key is then compared with a previous soft key to confirm that no change has occurred.

In contrast to the above confirmation of the integrity of the device, the present invention uses a serial flash memory module for updating a validator where the flash memory module contains operating software for the validator which has been encrypted. It is not desirable to have the serial flash memory module specific to the validator as there can be many validators in the field and the precise serial numbers of those to be updated may not be known. A potential problem is that the operating software for updating of the validator may have been tampered with, therefore, the present invention provides in the serial flash memory module the particular arrangement for confirming the authenticity thereof. Previously manufactured validators already have encryption software for interpreting the provided encrypted operating software but before updating of the validator will use the identification code provided in the read only memory which is also encrypted within the operating software. With this arrangement, the validator can perform the security check and only update to the new operating software if the appropriate confirmation occurs.

The reference of Meyer et al. is directed to a different principle, operates in a different manner and does not have the required elements set out in the claim. The Examiner's position that this soft key can subsequently be used for encrypting any information including the serial number is irrelevant given that this encryption would not be in the serial flash memory module nor would it be part of the encrypted operating software contained in the rewritable memory of the serial flash memory module.

REJECTION UNDER 35 U.S.C. 103

Applicant submits the references are incompatible, fail to teach or suggest the combination, and in addition, even if improperly combined, do not result in the structure as claimed.

The apparatus and method of the present application allows updating of a validator without communication to a central server or other remote secure device. The validator, together with an authentic removable memory storage arrangement, allows secure updating of the validator. Validators are often standalone devices used in vending machines or other devices with do not have external communication capabilities. Older validators with obsolete software can become effective if updated, to take into account new banknotes or new techniques to detect and reject fraudulent banknotes. Security of both the algorithms of the software of the flash memory device and the software of the validators is of high importance and will be evaluated by criminals for possible vulnerabilities. Full communication to a central server which maintains software and only downloads the information after confirmation of the validator's identity, is a desirable secure arrangement but is cost prohibitive for many validator applications where two way communication is not present or practical and requires skilled technicians to provide this communication capability.

The primary reference requires full two way communication with a remote server which is not necessary with the present system. The secondary reference has no security. Combining the references results in a full two way communication network linking the validator with a remote server.

A banknote validator according to the present invention has a series of sensors for scanning of a banknote as it moves

past the sensors. A central processing unit controls the operation of the validator and receives and processes the signals from the sensors. The validator includes a removable memory storage arrangement which is insertable in a receiving location of the validator. This removable memory storage arrangement when received in the receiving location, forms an electrical communication path with the central processing unit.

The central processing unit has a testing procedure which evaluates the integrity of any received removable memory storage arrangement. The central processing unit only downloads information from the storage arrangement upon a positive evaluation of the integrity of the removable memory storage arrangement. The removable memory storage arrangement includes an electronic address which is received by the central processing unit. The removable flash memory module contains encrypted algorithms used by the central processing unit to evaluate banknotes and the central processing unit includes decryption software for decoding the algorithms and storing the coded algorithms in the central processing unit. This electronic address is used by the central processing unit to determine the authenticity of the removable memory storage arrangement.

With the above arrangement, a standalone banknote validator installed in a vending machine or other device can easily be updated by merely inserting the removable flash memory module into the appropriate port of the validator. The validator decrypts the material and evaluates the integrity of the removable flash memory module to determine whether it is authentic. If the evaluation is positive, the software of the validator is updated. With this arrangement, there is no requirement for the removable flash memory module to know the serial number or address information of the validator. The

validator conducts its own evaluation of the integrity of the removable flash memory module based on information provided to it by the removable flash memory module.

In the preferred embodiment of the invention, as described on page 5 of the present application, the CPU obtains the identification code of the flash memory module from the read only memory of the flash memory module. The CPU decodes the information provided to it and part of the decoded information contains the identification code of the removable flash memory module. If there is an agreement between these two numbers, it is assumed by the CPU that the software is authentic and has not been exposed to corruption.

From the above, it can be appreciated that the evaluation carried out by the validator is based on information provided to it by the removable flash memory module. The validator receives the information from the module and based on the information provided, conducts a test of the module's integrity. Neither the primary reference nor the secondary references operate in this manner.

It is acknowledged in the Official Action that the primary reference of Mazur et al., does not include any separate evaluation of the integrity of the flash card that is used in the validator. Furthermore, there is no teaching that the removable memory module should have the software thereof encrypted to maintain the integrity of the system, nor does the CPU of the Mazur et al. reference have any capability of decrypting information.

The secondary reference of Meyer et al., is directed to an intelligent public telephone system and method. This patent

is classified in international class H04M17/00 or U.S. class 379, subclass 145.

The primary reference of Mazur is in international class G07D7/12 or U.S. class 194, subclass 207; class 382, subclass 135.

It is noted that none of the international or U.S. classes overlap between these references and there is no overlap between the fields of search with respect to each of these references.

It is submitted that these are not analogous art as confirmed by the completely different international and U.S. classes and is further confirmed by the various classes that were searched.

It is further noted that the intelligent public telephone systems and methods of the secondary reference of Meyer et al. is indeed remote and distinct from banknote validators associated with the testing of banknotes for either acceptance or rejection of the banknote in a currency transaction. It is submitted that it is only based on hindsight and with full knowledge of the present application that one would ever consider the secondary reference of Meyer et al. It is therefore argued that a person skilled in the art would not make this combination and there is no suggestion in either of these references to make the combination.

The Examiner asserts that the secondary reference of Meyer et al., uses a removable flash memory card in association with currency handling devices. It is believed this seriously mischaracterizes the Meyer et al. reference. The Meyer et al.

reference is directed to a fully integrated public telephone system and the flash memory referred to in the Meyer et al. patent is hardwired and integral with the telephone. It is not a removable device and as will be subsequently discussed, all updating of the Meyer et al. device occurs over the public telephone system as discussed according to the security arrangement disclosed in the patent.

The security arrangement clearly uses information associated with the actual telephone device, i.e., the electronic address of the telephone device as opposed to using any information which is inherent to a removable flash memory card. In fact, the Meyer et al. reference does not have a removable flash memory card and the only issue is whether the information that is downloaded to it over the public telephone system is authentic and appropriate for the particular telephone. The evaluation conducted according to the secondary reference is whether this firmware is appropriate for that particular device and is based on information specific to the telephone device with the remote computer making this determination, not the telephone device.

The Official Action on page 8 states as follows:

"At the time of the invention, it would have been obvious to one of ordinary skill in the art to have used the encryption scheme and flash memory card of Meyer et al in the bill handling system of Mazur et al.

The suggestion/motivation would have been to use a flash memory card to "promote product firmware security and configuration control".

Applicant submits this position disregards the teaching of the references.

The secondary reference of Meyer et al. teaches a security arrangement which allows an intelligent telephone with a hardwired flash memory device 5 (see Figure 1) to receive new "firmware" provided to it by the "management system". The telephone is designed to receive and to transmit voice and other communications and the telephone is designed to communicate with the telephone management system from time to time. The Board's attention is directed to column 6, lines 28 through 33 where it states:

"The telephone is designed to communicate with the phone management system via a proprietary 1200 baud FSK algorithm. Typically, modem communication is used to poll the installed telephone record, call accounting, and diagnostic information, or for downloading program, rating, or system configuration information."

Column 6, lines 61 to the bottom of the page further describes the primary system component systems of the telephone. It states:

"The primary system memory components are the utility FLASH 5 and data SRAM 6. The phone always boots up from the utility FLASH. The utility FLASH is a downloadable device containing boot code, standard utilities, and voice data. The data SRAM typically contains call rating information, as well as collected call records. Any of these typical uses may vary by firmware design."

It is apparent from these passages that the FLASH 5 is a downloadable device and is capable of receiving software sent to it over the telephone system from the central office to the particular telephone. This is not a removable memory module inserted into a validator for updating thereof with its own security structure.

Programming of the FLASH ROM is further described in column 16, lines 37 through 47. Programming of this ROM requires a proprietary interface box and this interface box initiates communication when its switch is turned on but the telephone's microprocessor will work as the master. Basically, the FLASH ROM can receive or has received new firmware for downloading. If this is the case, the device undergoes a security check. Column 17 states:

"To provide for the security required as well as allowing flexibility in implementation, three parameters will be required. The three parameters include configuration code, product code, and revision level."

The purpose of the configuration code is to match the specific group of firmware with the mother board's DS2502. As can be appreciated, the DS2502 is an inherent characteristic of the telephone and is not associated with a removable memory module. A second process is carried out to evaluate information of the DS2502 and an insertable key at JS. Once again, the security check is based on the characteristics of the mother board of the specific telephone.

The product code is subsequently discussed and is a code which is maintained by the mother board's DS2502. If the product

code of the DS2502 does not match with the provided product code, then the telephone will continue to operate in its normal manner.

A careful reading of column 17 and in consideration of Figures 17, 18 and 19, it is submitted that the security check provided in the secondary reference is based on information stored in and particular to the telephone and removable flash memory. Software is downloaded from the central office to the particular telephone. The telephone, then based on information specific to the telephone, is used to evaluate the provided software.

It is clear from the secondary reference that a fully networked system is necessary where the particular device is in full communication with a host office. Furthermore, the security system of this reference requires the particular device to review its own characteristics and conduct its test based on its determined characteristics and information downloaded to it.

The secondary reference is thus in direct contradiction to the present system. It is not practical to have validators which are fully networked. Networking of the validators is not required with the present invention.

It is respectfully submitted that even if the references were combined, they would not arrive at the invention as now claimed. It is critical, according to the secondary reference, to have a fully networked system. There is an integration between the intelligent telephone and the central office. The telephone is provided with a downloadable flash memory which can receive updates from the central office. Any new software which is received by the intelligent telephone is tested based on characteristics specific to the telephone.

If one was to combine this with the primary reference, it is respectfully submitted you would end up with a validator which is networked with the central office. In this way, the security system as taught by the secondary reference could be fully utilized. It is readily apparent that this solution is in contradiction to the system presently being claimed.

Even if one was to assume that the flash card of the primary reference should be secure as used in the downloadable memory of the secondary reference, this security would be based on the configuration code, product code and revision level as taught by the secondary reference. Therefore, the security arrangement would require full knowledge of the "configuration code, product code and revision level" of the validator in which the flash memory card was to be used. As indicated in the secondary reference, these are typically unique codes based on the serial numbers provided on the mother boards of the receiving device. This is in direct contradiction to the claimed invention where the validator merely evaluates and determines the suitability of the flash memory provided to it.

Such as system, which requires full knowledge of the particular validator to be updated, would not be satisfactory. This would require a direct pairing of the removable flash memory device with a particular validator using the specific information of the validator. This does not provide an easy system to update and requires a very efficient and accurate databank of serial numbers, processors, product codes, etc., covering many years. Also, the flash memory validator arrangement would be useable with only one validator as opposed to any validator which can confirm authenticity. Validators and vending machines move, and fully tracking thereof is not practical.

In contrast, the invention as claimed merely confirms that the software provided to the validator has not been tampered with based on the information provided with the removable memory module and the CPU of the validator then downloads the information after it has decrypted the information. If the validator cannot confirm the authenticity, the software may have been tampered with or the software was not designed for this type of validator. In either event, the validator is not updated. The prior art references do not even suggest such a system. Any further modification of the primary and secondary reference would be in direct contradiction to the principles set out in these references.

As previously argued, the primary reference has promoted the benefits of the module being capable of being used with many validators and has not appreciated how this arrangement can render the entire system subject to attack or vulnerable. With the present system, all critical information provided in the removable memory module is encrypted and thus, the techniques used by this software to determine the authenticity of banknotes is extremely difficult to determine. This encryption of the software has also encrypted preferably the address of the removable serial module and the validator uses this information as part of its integrity test. If any tampering has occurred to the removable memory module, there will not be a match and the validator will continue to operate in its normal mode.

Method claim 19 has been amended to include the additional step of dependent claim 20. The method of updating the bank validator as set out in claim 19, requires coordination between the removable sensor modules and the removable memory storage arrangement. The claim requires the validator to carry

out an evaluation of the updated information prior to installing thereof.

This claim was rejected in view of Mazur et al. in view of Itako et al. and further in view of Meyer et al.

As previously argued, Meyer et al. is not directed to the currency validating art. Therefore, the arguments previously submitted regarding the combination of the primary reference and Meyer et al. are reasserted.

It is further argued that there is no teaching to combine the references in this manner. The primary reference has fixed sensors whereas the secondary reference teaches sensors which are movable within the device. The third reference teaches encryption over a networked system using information specific to the telephone provided by the telephone to a central office which then downloads the information.

The encryption and security technique required of the method claim is not found in the combination and it is again asserted that the only teaching or suggestion for combining the references in this manner is found in the disclosure of the present case. This hindsight analysis and merely using the present disclosure and claims as a road map to selectively identify individual elements to be combined without any suggestion in the references to make this combination is not the appropriate test of obviousness.

The telephone system of the Meyer et al. reference operates on an entirely different basis requiring a complete network system and security being provided by a central office. This is in contrast to a validator which in many cases will be

located in a vending machine or device with no ability to communicate to a central source.

The rejection of claims 1 through 20 under the judicially created doctrine of obviousness-type double patenting is traversed. U.S. Patent 6,142,284 does not have a validator adapted to receive a removable memory module. It only teaches removable sensor modules. The secondary reference of Meyer et al. discloses a telephone and a security system for the telephone as it interacts with a central office. Neither reference has a removable memory module nor the cooperation of the validator and the memory module using information inherent to the memory module.

It is therefore submitted this rejection be withdrawn.

Obviousness is determined by "what the combined teachings of the references would have suggested to those of ordinary skill in the art". *In re Keller*, 208 USPQ 871, 881. Obviousness "cannot be established by combining the teaching of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination" and "teachings of references can be combined only if there is some suggestion or incentive to do so." *ACS Hosp. Sys., Inc. v. Montefiore Hosp.*, 221 USPQ 929, 933.

"To imbue one of ordinary skill in the art with the knowledge of the invention in suit, when no prior art reference or references of record convey or suggest that knowledge, is to fall victim to the insidious effect of a hindsight syndrome wherein that which only the inventor taught is used against its teacher." *W.L. Gore & Assoc. v. Garlock, Inc.*, 721 F.2d 1540, 1553, 220 USPQ 303, 312 (Fed. Cir. 1983).

"In order to establish obviousness, it is necessary for the examiner to present evidence, preferably in the form of some teaching, suggestion, incentive or inference in the applied prior art, or in the form of generally available knowledge, that one having ordinary skill in the art would have been led to combine the relevant teachings of the applied references in the proposed manner to arrive at the claimed invention." *Ex parte Levengood*, 28 USPQ2d 1300, 1301.

"The question is not whether a patentable distinction is created by viewing a prior art apparatus from one direction and a claimed apparatus from another, but, rather, whether it would have been obvious from a fair reading of the prior art reference as a whole to turn the prior art apparatus upside down. French teaches a liquid strainer which relies, at least in part, upon the assistance of gravity to separate undesired dirt and water from gasoline and other light oils. Therefore, it is not seen that French would have provided any motivation to one of ordinary skill in the art to employ the French apparatus in an upside down orientation. The mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification." *In re Gordon*, 221 USPQ 1125, 1127.

"In this case, however, the only suggestion for the examiner's combination of the isolated teachings of the applied references improperly stems from appellant's disclosure and not from the prior art. *In re Ehrreich*, 590 F.2d 902, 200 USPQ 504 (CCPA 1979). At best, the examiner's comments regarding obviousness amount to an assertion that one of ordinary skill in the relevant art would have been able to arrive at the appellant's invention because he had the necessary skills to

carry out the requisite process steps. This is an inappropriate standard for obviousness. See *Orthokinetics Inc. v. Safety Travel Chairs Inc.*, 806 F.2d 1565, 1 USPQ2d 1081 (Fed. Cir. 1986). That which is within the capabilities of one skilled in the art is not synonymous with obviousness. *Ex parte Gerlach*, 212 USPQ 471 (Bd.App. 1980). See also footnote 16 of *Panduit Corp. v. Dennison Mfg. Co.*, 774 F.2d 1082,1092, 227 USPQ 337,343 (Fed. Cir. 1985). That one can *reconstruct* and/or explain the theoretical mechanism of an invention by means of logic and sound scientific reasoning does not afford the basis for an obviousness conclusion unless that logic and reasoning also supplies sufficient impetus to have led one of ordinary skill in the art to combine the teachings of the references to make the claimed invention. ... Accordingly, an examiner cannot establish obviousness by locating references which describe various aspects of a patent applicant's invention without also providing evidence of the motivating force which would impel one skilled in the art to do what the patent applicant has done." *Ex parte Levengood*, 28 USPQ2d 1300, 1301.

For the above reasons, it is believed that the combination relied on by the Examiner does not include the cooperation of the components, let alone render the claimed structure obvious. The combined references fail to teach the required validator which receives and evaluates a coded removable memory storage arrangement prior to updating the operation system of the validator.

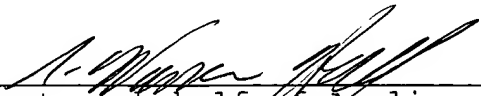
It is further submitted that the teachings of the present application have been improperly used as a selection criteria for combining the prior art and seeking disclosure of individual elements without any rationale for combining these diverse references in a manner in contradiction to the teachings of the individual references. There is no teaching or suggestion

in the references to seriously modify the structures in contradiction to the teaching thereof in an attempt to arrive at the combination claimed.

Applicant submits that the references when considered in their entirety, do not set forth a *prima facie* case that the claims are obvious. There is no rationale when one considers the references in their entirety why a person skilled in the art would have been led to the claimed invention by the express teachings or suggestions found in the prior art. The claimed invention should be considered as a whole and in the present application, there is a unique combination of components which cooperate to provide secure, cost effective, updating of a validator by an end user. This is in contradiction to each of the references which in one case has no security and in a second case uses a remote computer to obtain information specific to a telephone before updating thereof. These prior art systems are not cost effective or appropriate for updating validators.

A copy of the appealed claims is attached.

In view of the above, it is requested that the rejection of the claims be reversed.



Agent on behalf of Applicant
S. Warren Hall
Reg. No. 30,350
(416) 368-8313

WH/sdw
Encls.

APPEALED CLAIMS

1. A banknote validator comprising a banknote processing channel, a series of sensors located along said channel for scanning a banknote as it moves past said sensors, a central processing unit for controlling the operation of said validator and receiving and processing the signals from said sensors, and a removable memory storage arrangement insertable in a receiving location of said validator, said removable memory storage arrangement when received in said receiving location forming an electrical communication path with said central processing unit, said central processing unit including a testing procedure which evaluates the integrity of any received removable memory storage arrangement and said central processing unit downloading information from said received removable storage arrangement for operation thereof upon positive evaluation of the integrity of said removable memory storage arrangement.

2. A banknote validator as claimed in claim 1 wherein said removable memory storage arrangement is a serial flash memory module.

3. A banknote validator as claimed in claim 1 wherein the removable memory storage arrangement includes an electronic address available to the central processing unit and the electronic address is used to confirm the encoded so.

4. A banknote validator as claimed in claim 2 wherein said central processing unit of the validator will not allow the validator to operate if the central processing unit has previously downloaded information

from a serial flash memory module and a serial flash memory module is not received in said validator.

5. A banknote validator as claimed in claim 3 wherein the removable flash memory module contains encrypted algorithms used by the central processing unit to evaluate banknotes for authenticity and the central processing unit includes decryption software for decoding the algorithms and storing the decoded algorithms in said central processing unit.

6. A serial flash memory module for updating a validator comprising a read only memory which includes an identification code specific to the serial flash memory module and a rewritable memory containing encrypted operating software for operating a validator, said encrypted software including encryption of at least part of said identification code.

8. A banknote validator as claimed in claim 3 wherein said removable memory storage arrangement provides additional memory available to said central processing unit for evaluation of banknotes.

10. A banknote validator as claimed in claim 1 wherein said removable memory storage arrangement contains encrypted algorithms used by the central processing unit to evaluate banknotes for authenticity.

11. A banknote validator as claimed in claim 1 wherein said validator includes an electronic address available to said central processing unit, and said removable memory storage arrangement includes a memory location for storing the electronic address of the validator when received in said removable storage arrangement.

12. A banknote validator as claimed in claim 2 wherein said serial flash memory module contains information to be downloaded to said central processing unit for controlling the operation of said validator, said serial flash module after downloading of said information including a security feature such that said serial flash module can not be used with other validators.

13. A banknote validator as claimed in claim 11 wherein said serial flash memory module records the electronic address of the validator when received in said receiving arrangement and only communicates with said central processing unit when there is a match between the recorded electronic address and the electronic address provided by the validator.

14. A banknote validator as claimed in claim 1 wherein said removable memory storage arrangement provides additional memory available to said central processing unit for evaluation of banknotes.

15. A banknote validator as claimed in claim 2 wherein said removable memory storage arrangement contains encrypted algorithms used by the central processing unit to evaluate banknotes for authenticity.

16. A banknote validator comprising a banknote processing channel, a series of removable sensors located along said channel for scanning a banknote as it moves past said sensors, a central processing unit for controlling the operation of said validator and receiving and processing the signals from said sensors, and a receiving location for receiving a removable memory storage arrangement and forming an electrical

communication path with said central processing unit, and wherein said banknote validator can be updated by replacing at least some of said removable sensors with new removable sensors and updating said central processing unit to operate with said new sensors by downloading banknote processing information from said received removable memory storage arrangement.

17. A banknote validator as claimed in claim 16 wherein said downloaded banknote processing information is specific to said new removable sensors.

18. A banknote validator as claimed in claim 16 wherein said removable sensors include a series of removable sensor modules and each sensor modules includes at least one sensor.

19. A method of updating the criteria used to evaluate the authenticity of banknotes by a banknote validator having a banknote processing channel, a series of removable sensor modules located along said channel for scanning a banknote as it moves past said sensor modules, a central processing unit for controlling the operation of said validator and receiving and processing the signals from said sensor modules, and a receiving location for receiving a removable memory storage arrangement and allowing communication between said central processing unit and a received removable memory storage arrangement, said central processing unit including a testing procedure which evaluates the integrity of any received removable memory storage arrangement, said method comprising inserting a removable memory storage arrangement in said receiving arrangement and communicating with said central processing unit, conducting said test procedure using information provided to said central processing

unit by said removable memory storage means to confirm the integrity thereof, and in response to confirmation of the integrity of said removable memory storage arrangement downloading information contained in said removable memory storage arrangement to said central processing unit thereby updating the criteria used to evaluate banknotes processed by the validator.

20. A method as claimed in claim 19 including the step of replacing at least one of the sensor modules with a new sensor module and wherein said central processing unit is updated to process the signal of said at least one new sensor module using said downloaded information.